UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,827	01/17/2001	Ronald P. Doyle	RSW92001008US1	6499

7590 07/30/2004

Jeanine S. Ray-Yarletts
IBM Corporation
T81/503
P. O. Box12195
Research Triangle Park, NC 27709

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	6

DATE MAILED: 07/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/764,827	DOYLE ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2001* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-105* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-105* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *4,5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Pursuant to USC 131, claims 1-105 are presented for examination.

Specification

2. The disclosure is objected to because of the following informalities: on page 1, the related patent applications have no serial numbers. Applicant is required to add the following patent numbers: on page 8, line 8 US Patent "6772331". Appropriate correction is required.

2.1 The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

2.2 The abstract of the disclosure is objected to because it contains the term "the disclosed techniques". Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

2.3 The disclosure is objected to because it contains embedded hyperlinks and/or other form of browser-executable codes (see page 4, line 16; and page 29, line 7). Applicant is required to delete the embedded hyperlinks and/or other form of browser-executable codes. See MPEP § 608.01.

2.4 The use of the trademark "WORKPAD" and "PALMPILOT" has been noted in this application, for instance on page 2, lines 16-18. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Objections

3. **Claims 10, 42, and 65**, are objected to because of the following informalities: on lines 2 and 3, "hardware reset of the component" and operably connecting of the component needs to be revised. There is lack of antecedent basis for these claims. Appropriate correction is required.

3.1 **Claim 105** is objected to because it is substantial duplicate of another claim. Applicant is advised that should **claim 103** be found allowable, **claim 105** will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in

wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 26-27, 60-61, and 94-95 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4.1 Regarding **claims 26-27, 60-61, and 94-95,** the phrase "the security core" renders the claim(s) indefinite because the claim(s) include(s) elements not actually disclosed (those encompassed by " the security core "), thereby rendering the scope of the claim(s) unascertainable. There is no antecedent basis the phrase "the security core".

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5.1 Claims 1, 35, and 69 and 104, provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-2, 56-57, and 33-34 respectively of copending Application No. 09/764844 in view of US Patent 5,229,764 to Matchett et al.. The difference between the present Application and the copending Application is repeatedly obtaining biometric input of a user; comparing the repeatedly obtaining biometric input wherein each comparison comprises an authentication of the user. Matchett et al. reference discloses "a continuous biometric authentication for the purpose of security and protection of any system or device such that continued use of the protected system or device is directly dependent upon continued passing of biometric tests according to a preselected threshold of acceptability". It would have been obvious to one skilled in the art to repeatedly obtain biometric input of a user to enhance security as taught by Matchett et al. for all the reasons disclosed by Matchett et al. such as "if biometric checks are increased in duration and/or number, security would be enhanced and user substitution to an unauthorized user would be prevented".

This is a provisional obviousness-type double patenting rejection.

5.2 Claims 103 and 105 provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 56-57 and 73 of copending Application No. 09/764844 in view of US Patent 5,229,764 to Matchett et al.. The difference between the present Application and the copending Application is repeatedly obtaining biometric input of a user; comparing the repeatedly obtaining biometric input wherein each comparison

comprises an authentication of the user. Matchett et al. reference discloses "a continuous biometric authentication for the purpose of security and protection of any system or device such that continued use of the protected system or device is directly dependent upon continued passing of biometric tests according to a preselected threshold of acceptability". It would have been obvious to one skilled in the art to repeatedly obtain biometric input of a user to enhance security as taught by Matchett et al. for all the reasons disclosed by Matchett et al. such as "if biometric checks are increased in duration and/or number, security would be enhanced and user substitution to an unauthorized user would be prevented".

This is a provisional obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 **Claims 1-29, 33-63, 67-97, 101-105** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,125,192 to **Bjorn et al.** in view of US Patent 5,229,764 to **Matchett et al.**.

6.2 **As per claims 1, 17-19, 35, 51-53, 69, 85-87, and 104, Bjorn et al.** substantially teaches a method and system for providing continuous authentication of a user of a computing device, comprising: a security component which provides security functions, such that the security component can vouch for authenticity of one or more components with which it is securely operably connected, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27); a biometric sensor component that is securely operably connected as one of the one or more other components to the security component, for example (see column 4, line 39 through column 5, line 22; see also column 5, line 43 through column 6, line 27 and column 4, line 39 through column 5, line 22); securely-stored biometric information which identifies an owner of the computing device, for example (see column 4, line 39 through column 5, line 22 and column 6, lines 18-27); means for obtaining from the biometric sensor component biometric input of a user of the computing device and means for comparing the obtained biometric input to the securely-stored biometric information of the owner, for example (see column 6, lines 27-43).

Matchett et al. in an analogous art teaches means for repeatedly obtaining from the biometric sensor component such as fingerprint sensor, retinal scan etc., for example (see column 1, lines 60-67) biometric input of a user of the computing device and means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each comparison comprises an authentication of the user, for example (see column 3, lines 10-55). **Matchett et al.** discloses that if biometric checks are increased in duration and/or number, security would be enhanced and user substitution to an unauthorized user would be prevented, for example (see column 2, lines 55-66). Therefore, it would have

been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of **Bjorn et al.** to provide teaches means for repeatedly obtaining from the biometric sensor component biometric input of a user of the computing device and means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each comparison comprises an authentication of the user as taught by **Matchett et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Matchett et al.** so as to enhance security and prevent user substitution to an unauthorized user, for example (see column 2, lines 55-66).

As per claims 2, 33, 36, 67, 70, and 101, Matchett et al discloses the limitation of wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation, for example (see column 3, lines 10-55). Therefore, these claims are rejected on the same rationale as the rejection of claims 1, 35, and 69.

As per claims 3-4, 37-38, and 71-72, Matchett et al discloses the limitation of wherein the means for repeatedly obtaining is activated each time a predetermined time interval elapses and wherein the predetermined time interval is selectively configured by the owner of the computing device for example (see column 3, lines 10-55 and column 7, lines 2-35). Therefore, these claims are rejected on the same rationale as the rejection of claims 1, 35, and 69.

As per claims 5-6, 8, 39-40, 42, and 73-74, 76, Matchett et al discloses the limitation of wherein the means for repeatedly obtaining is activated upon switching between functions of an application that is executing a security-sensitive operation using the computing device, and wherein the means for repeatedly obtaining is activated upon reaching one of at least one predetermined instructions in an application that is executing a security-sensitive operation using the computing device, for example (see column 3, lines 10-55 and column 10, line 35 through column 11, line 22). Therefore, these claims are rejected on the same rationale as the rejection of claims 1, 35, and 69.

As per claims 7, 41, and 75, Matchett et al discloses the limitation of wherein the means for repeatedly obtaining is activated when the biometric sensor component detects one or more of an interruption, change, or loss of the biometric input, for example (see column 3, lines 10-55 and column 7, lines 18-28). Therefore, these claims are rejected on the same rationale as the rejection of claims 1, 35, and 69.

As per claims 9, 43, and 77, Bjorn et al. discloses the limitation of wherein selected ones of the secure operable connections are provided when the security component is manufactured, for example (see column 9, lines 52-62).

As per claims 10, 44, and 78, Bjorn et al. discloses the limitation of wherein the components comprise one or more of (1) input/output components and (2) application processing components, for example (see column 8, lines 4-30).

As per claims 11-12, 14-15, 28, 45-46, 48-49, 62, 79-80, 82-83, and 96, Bjorn et al. discloses the limitation of wherein the means for securely operably connecting further comprises means for authenticating the biometric sensor to the security component and means for authenticating the security component to the biometric sensor, for example (see column 9, line 30 through column 10, line 7) and security handshake, for example (column 6, lines 52-65). **Bjorn et al.** discloses the limitation of wherein the means for authenticating the biometric sensor securely stored thereon.

As per claims 13, 47, and 81, Bjorn et al. discloses the limitation of wherein the means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component, for example (see column 8, lines 4-30).

As per claims 16, 50, and 84, Bjorn et al. discloses the limitation of further comprising means for concluding that the user is the authorized holder of the card only if the means for comparing succeeds, for example (see column 6, lines 27-43 and column 16, line 50 through column 17, line 5).

As per claims 20, 54, and 88, Bjorn et al. discloses the limitation of further comprising means for securely transferring the stored biometric information of the authorized holder to the biometric sensor for use by the means for comparing, for example (see column 6, lines 28-43 and column 17, lines 50-67).

As per claims 21, 55, and 89, Bjorn et al. discloses the limitation of wherein the means for comparing is performed by the security component, for example (see column 8, line 60 through column 9, line 3).

As per claims 22, 56, and 90, Bjorn et al. discloses the limitation of further comprising means for aborting the security-sensitive operation if the means for repeatedly obtaining or the means for comparing fails to detect the biometric information of the user thereby causing the completion of the security-sensitive operation, for example (see column 9, lines 4-25; column 10, lines 15-21; and column 16, line 44 through column 17, line 23).

As per claims 23-25, 57-59, and 91-93, Bjorn et al. discloses the limitation of further comprising means for aborting the security-sensitive operation, means for marking the sensitive operation as not authenticated, means for deactivating the computing device, if the means for repeatedly obtaining or the means for comparing fails to detect the biometric information of the user; and means for concluding that the security-sensitive operation is authentic if the means for comparing succeeds until completion of the security-sensitive operation, for example (see column 9, lines 4-25; column 10, lines 15-21; and column 16, line 44 through column 17, line 23).

As per claims 26-27, 60-61, and 94-95, Matchett et al discloses the limitation of wherein the means for concluding that the security-sensitive operation is authentic also requires that all other components which are securely operably connected to the security core and which

are involved in the security-sensitive operation remain connected until completion of the security-sensitive operation, for example (see column 10, lines 2-10). Therefore, these claims are rejected on the same rationale as the rejection of claims 1, 35, and 69.

As per claims 29, 63, and 97, Bjorn et al. discloses the limitation of wherein the biometric sensor component has associated therewith a unique device identifier that is used to identify data originating therefrom, a digital certificate, a private cryptographic key and a public key cryptographically associated with the private key, for example (see column 9, line 30 through column 10, line 45).

As per claims 34, 68, and 102, Bjorn et al. discloses the limitation of wherein the means for authenticating further comprises means for using a unique device identifier of the biometric sensor, a digital signature computed over the unique identifier using a private key of the sensor, a private cryptographic key and a public key cryptographically associated with the private key, for example (see column 9, line 30 through column 10, line 45).

Claims 103 and 105 contain the limitations found in the rejected **claims 1, 35, 69, and 104 and claim 56**. Therefore, **claims 103 and 105** are rejected on the same rationale as the rejection of **claims 1, 35, 69, and 104 and claim 56**.

7. **Claims 30-32, 64-66, and 98-100** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,125,192 to **Bjorn et al.** in view of US Patent 5,229,764 to

Matchett et al. as applied to claims 1, 35, and 69 above, and further in view of US Patent 6,325,285 to **Baratelli**.

7.1 **As per claims 30-32, 64-66, and 98-100,** both references substantially teach sensor and security card. **Bjorn et al.** also discloses the limitation of wherein the previously-stored secrets include a private cryptographic key of the authorized holder, and wherein the means for accessing further comprising means for accessing the private key to compute a digital signature over information presented to the card, for example (see column 9, line 30 through column 10, line 45). **Matchett et al.** also discloses integrated the invention into a compact, portable device, for example (see column 9, lines 50-55) and also uses other embodiments of integrating a sensor with protected device for continuous authentication and further discloses in prior art that a problem with a smart card is that it may be stolen. It would have been obvious to one skilled in the art to integrate the sensor with a card as to provide continuous authentication as suggested by **Matchett et al.**. **Baratelli** in an analogous art teaches biometric sensor physically integrated with a card and wherein a card reader adapted to reading the card is securely operably connected to the security component, for example (see abstract). **Baratelli** also discloses previously-stored secrets of the owner of the computing device and means for accessing selected ones of the previously-stored secrets only if the means for comparing determines that the obtained biometric information of the user matches the stored biometric information of the authorized holder, for example (see column 7, lines 5-27) and wherein the previously-stored secrets include a private cryptographic key of the authorized holder, and wherein the means for accessing further comprising means for accessing the private key to compute a digital signature over information

presented to the card, for example (see column 7, lines 27-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system as combined above to physically integrate the sensor with a card as taught by **Baratelli** for continuous authentication s suggested by **Matchett et al.**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Baratelli** in order to provide security and prevent user substitution to an unauthorized user, for example (see column 2, lines 55-66) without departing from the spirit and scope of the invention by **Matchett et al.**.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin
Patent Examiner
July 23, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100